TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

AUTENTIZACE UŽIVATELŮ PRO VZDÁLENÝ PŘÍSTUP DO POČÍTAČOVÉ SÍTĚ LIANE PŘI ZTRÁTĚ HESLA

Bakalářská práce

Studijní program: B2646 – Informační technologie
Studijní obor: 1802R007 – Informační technologie

Autor práce: **Roman Belda**
Vedoucí práce: Ing. Lenka Kosková - Třísková

Liberec 2014

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Mechatronics, Informatics
and Interdisciplinary Studies

LIANE NET REMOTE ACCESS USER AUTHENTICATION IN CASE OF A PASSWORD LOSS

Bachelor thesis

Study programme: B2646 – Information Technology
Study branch: 1802R007 – Information Technology

Author: **Roman Belda**
Supervisor: Ing. Lenka Kosková - Třísková

Liberec 2014

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky a mezioborových studií
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Roman Belda**
Osobní číslo:	**M12000106**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Autentizace uživatelů pro vzdálený přístup do počítačové sítě LIANE při ztrátě hesla**
Zadávající katedra:	**Ústav nových technologií a aplikované informatiky**

Zásady pro vypracování:

1. Seznamte se sáteoretickými metodami autentizace do počítačových systémů a možností jejich kombinací.
2. Proveďte analýzu rizik a použitelnosti jednotlivých metod vápřípadě nasazení váprostředí počítačové sítě LIANE.
3. Proveďte rešerši systémů autentizace do počítačových sítí nejméně dvou velkých univerzit, analyzujte tato řešení záhlediska použitelnosti a bezpečnosti.
4. Proveďte analýzu všech používaných identifikačních nástrojů (karet) využívaných pro přístup kápočítačové síti LIANE.
5. Zaměřte se na ukládání a zpracování dat na jednotlivých kartách.
6. Navrhněte koncept autentizace do počítačové sítě LIANE bez použití uživatelského hesla, sávyužitím jiných nástrojů (karty a doplňkové metody).
7. Navrhněte prototypové zařízení, jež realizuje vámi navrženou metodu autentizace.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **cca 45 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] DOSEDĚL, T.: Počítačová bezpečnost a ochrana dat, Computer Press 2004, ISBN: 80-251-0106-1.
[2] LUDVÍK, M: Teorie bezpečnosti počítačových sítí, Computer Media 2008, ISBN: 8086686353.

Vedoucí bakalářské práce: **Ing. Lenka Kosková - Třísková**
Ústav nových technologií a aplikované informatiky

Datum zadání bakalářské práce: **21. října 2013**
Termín odevzdání bakalářské práce: **16. května 2014**

prof. Ing. Václav Kopecký, CSc.
děkan

L.S.

prof. Dr. Ing. Jiří Maryška, CSc.
vedoucí ústavu

V Liberci dne 21. října 2013

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum: 16.5.2014

Podpis: Balda Roman

Poděkování

Tímto bych rád poděkoval vedoucí mé bakalářské práce paní Ing. Lence Koskové Třískové za poskytnuté konzultace, užitečné rady a připomínky.

Rád bych poděkoval panu Petru Adamcovi z Oddělení pro správu sítě LIANE a panu Ing. Igoru Kopetschkovi, který spravuje karetní centrum, za rady a poskytnuté informace týkající se problematiky této bakalářské práce.

Dále bych chtěl poděkovat panu Ing. Janu Havlíčkovi z Vysoké školy ekonomické v Praze, panu Ing. Pavlu Poláčkovi z Univerzity Jana Evangelisty Purkyně a panu

Ing. Jiřímu Slaninovi z Univerzity Pardubice za jejich čas a poskytnuté informace.

V neposlední řadě děkuji své rodině za podporu během mého studia.

Abstrakt

Cílem této práce je navrhnout prototyp zařízení, které bude realizovat změnu centrálního hesla v případě jeho zapomenutí nebo ztráty. Po odborných konzultacích jsem navrhl způsob autentizace uživatelů s využitím identifikační čipové karty a jednorázového hesla, které bude odesláno formou SMS zprávy na mobilní telefon uživatele. Provedl jsem návrh hardwarového a softwarového vybavení zařízení. Dále jsem se v této práci věnoval porovnání způsobu přihlašovaní do univerzitních sítí na různých univerzitách v České republice.

Klíčová slova

Autentizace uživatele, identifikační karta, centrální heslo, ztracené/zapomenuté heslo

Abstract

The purpose of this study is to propose a device prototype that would be able to change the main password in case it is forgotten or lost. After expert consultations I have proposed a user authentication method that would use an ID chip card and a one-time password that would be sent to the user´s cell phone via a text message. I have presented hardware and software description of the device. Further, I drew a comparison between various universities in the Czech Republic regarding log in methods in use.

Keywords

User authentication, ID chip card, main password, lost/forgotten password

Obsah

Seznam zkratek

TUL	Technická univerzita v Liberci
LIANE	**LI**berec **A**cademic **NE**twork
tzn.	to znamená
atd.	a tak dále
SMS	Short Message Service (*Systém krátkých zpráv*)
VŠE	Vysoká škola ekonomická v Praze
UJEP	Univerzita Jana Evangelisty Purkyně v Ústí nad Labem
UPCE	Univerzita Pardubice
IS/STAG	Informační systém studijní agendy
EDUID	Česká akademická federace identit
OP	Občanský průkaz
ŘP	Řidičský průkaz
RADIUS	Remote Authentication Dial In User Service (*Uživatelská vytáčená služba pro vzdálenou autentizaci*)
VPN	Virtual private network
AD	Microsoft Active Directory
LDAP	Lightweight Directory Access Protocol
SMTP	Simple Mail Transfer Protocol
ISIS	Studijní informační systém
FAR	False Acceptance Rate (četnost povolení neoprávněného vstupu)

FRR	False Rejection Rate (četnost odmítnutí oprávněného vstupu)
SSO	Single sign-on
NFC	Near Field Communication (bezdrátová komunikace na krátkou vzdálenost)
GSM	Globální Systém pro Mobilní komunikaci
IC	Informační centrum
KC	Kartové centrum
CC	Copy centrum
PIN	Personal Identification Number (osobní identifikační číslo)

Seznam tabulek

Seznam obrázků

1 Úvod

Když uživatel zapomene nebo v horším případě ztratí, centrální heslo do sítě LIANE, má dnes k dispozici pouze jedinou možnost pro změnu hesla: osobní návštěvu na studijním oddělení, případně na Správě sítě LIANE, kde je uživateli vygenerováno nové přístupové heslo s omezenou platností.

V této práci jsem se věnoval přístupům jiných univerzit v České republice k přihlašování do univerzitních sítí. Řešil jsem vhodný koncept autentizace uživatele do počítačové sítě LIANE bez znalosti centrálního hesla.

Zařízení bude uživatelům k dispozici nepřetržitě. Jedná se o doplňkovou službu, kterou si každý uživatel může, dle svého uvážení, povolit.

Toto zařízení je možné do budoucna rozšířit o další funkce. Také je snadné zařízení do systému přidávat nebo odebírat.

2 Metody ověření uživatele

Uživatele je možné ověřit pomocí tří metod: **důkaz znalostí**, **důkaz vlastnictvím**, **důkaz vlastností**. [1]

2.1 Důkaz znalostí

Metoda vyžaduje po uživateli se prokázat znalostí tajné informace. Nejčastějším případem je znalost uživatelského jména a hesla. Uživatel je často nucen si pamatovat velmi složitá hesla. Tvar hesla, který například doporučuje webový portál LIANE je: *Jl:SpG03.* [2] Pokud uživatel není limitován délkou hesla, je vhodné použít úryvek básně pro lepší zapamatování. Důvodem proč máme využívat různé velikosti písmen, číslic nebo speciálních znaků je, že se snažíme zvýšit počet možných kombinací, které by potenciální útočník mohl použít.

Mnoho uživatelů se dopouští chyb, které plynou ze složitostí generovaných hesel. Poznamenávají si hesla do mobilních zařízení, nebo písemnou formou do bloků. Sice mají zvolené velmi bezpečné heslo, ale jejich uložení již neřeší. Může se stát, že mobilní telefon bude ukraden, a s tím i hesla k bezpečnostním schránkám, k bankovnímu účtu apod. Pro bezpečné ukládání hesel tedy doporučuji software zvaný KeePass. [3]

Obrázek 1: KeePass: free, open-source software

Jedná se o volně dostupný, otevřený software, který slouží k bezpečnému ukládání hesel. Je naprogramován pro většinu používaných operačních systémů. Databázi hesel je možné zaheslovat třemi způsoby:

1. centrální heslo
2. pomocí souboru (*.key), nebo s využitím souboru, který je použit jako klíč

3. V případě verze pro MS Windows 7 Home Edition je možné využít účet, kterým se přihlašují uživatelé do MS Windows.

2.1.1 Stávající situace na TUL

Důkaz znalostí funguje na Technické univerzitě v Liberci standardně. Využívá se uživatelské jméno ve tvaru: *jmeno.prijmeni*

V případě, že jsou na škole uživatelé se stejným jménem a příjmením přidává se na konec jejich uživatelského jména číslo: *jmeno.prijmeni1*

Centrální heslo nyní získávají studenti při slavnostní imatrikulaci. Do budoucna se plánuje, že studenti získají přístupové údaje ke svému účtu v dopise o vyrozumění přijetí na Technickou univerzitu v Liberci.[1] Účet jim bude aktivován po zápisu do ročníku.

Pomocí uživatelského jména a centrálního hesla mají studenti přístup: do počítačové sítě v učebnách; do Menzy; na e-learningový portál; na školní e-mail; k webovým stránkám, kde si mohou nastavit heslo pro vzdálený přístup; na kolejní webové stránky; k VPN připojení na univerzitu; na portál otevřená univerzita; do programu MSDN; do T-UNI diskuze; do studentské unie; na portál Moodle; a plno dalších systémů, které využívají pro ověření uživatele školní systém Shibboleth.

Obrázek 2: Logo softwaru Shibboleth

Jedná se o otevřený software, který poskytuje nástroj pro SSO (Single Sign-On). [4] To znamená, že uživatel se přihlásí pouze jednou do systému. A od této chvíle může přistupovat k různým WWW serverům, které tohoto uživatele rozpoznají.

1 Zdroj informace pan Petr Adamec.

2.1.2 Analýza rizik

Hlavním rizikem této metody je prozrazení uživatelského jména a hesla. Cizí osoba má přístup ke všem informacím o uživateli a může je dle libosti měnit, zneužívat apod. Proto je velmi důležité, aby uživatelé byli informováni o nebezpečnosti sdělování přihlašovacích informací.

2.2 Důkaz vlastnictvím

Metoda vyžaduje po uživateli vlastnit bezpečnostní předmět, který musí mít neustále při sobě. Tento předmět na Technické univerzitě v Liberci známe jako studentská čipová karta, ISIC, ITIC, čipová klíčenka. Nevýhodou této metody je, že v případě ztráty bezpečnostního předmětu může útočník využívat služby jménem majitele předmětu. Proto uživatel musí ihned při zjištění ztráty předmětu tuto ztrátu nahlásit na studijním oddělení případně na Správě sítě LIANE, která provede blokaci karty. Tato blokace karty se redistribuuje na další systémy, se kterými je spojena.

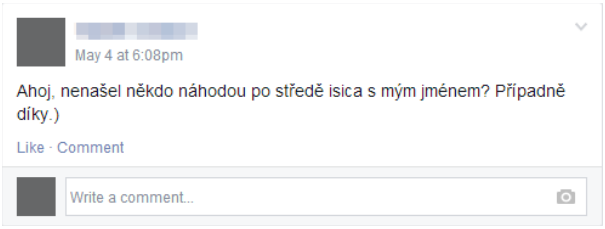
Seznam systémů, ke kterým je čipová karta připojena:

- přístup na všechny bloky kolejí – v případě, že je student ubytován
- výdej obědů (finanční konto pro obědy)
- aktivovaný tisk na tiskárnách SATIKOS (finanční konto pro tisk)
- možnost výpůjčky knih v Krajské vědecké knihovně Liberec (riziko náhrady škody, případné možné penále v případě nevrácení knihy)
- je možné na ISIC kartu nahrát Městské hromadné dopravy Liberec (finanční konto pro jízdu hromadnou dopravou)

Studenti o bezpečnostním riziku bezpečnostního předmětu nejsou dostatečně informováni. Neklade se na ztrátu bezpečnostního předmětu důraz. Osobně přirovnávám ztrátu ISIC karty ke ztrátě kreditní karty.

Obrázek 3 ilustruje, jak studenti zacházejí se ztrátou ISIC karty. Osobně jsem se

studentem hovořil. Potvrdil mi, že ISIC kartu nezablokoval, a čekal, než se ISIC karta objeví. Na konec ji úspěšně našel, bez žádné ztráty.



Obrázek 3: Příspěvky na sociální síti, v případě ztráty čipové karty

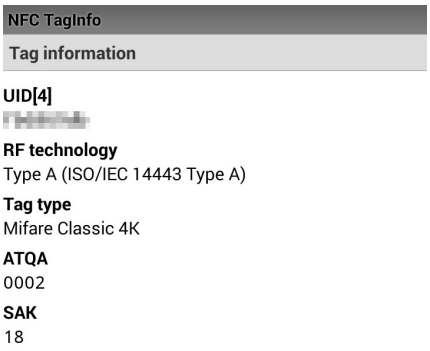
2.2.1 Stávající situace na TUL

Na Technické univerzitě v Liberci používáme několik čipových identifikačních předmětů. Jedná se o TUL čipové karty pro studenty a pedagogy. Poté ISIC a ITIC čipové karty pro studenty a pedagogy.

Obrázek 4: ISIC (vlevo) pro studenty a ITIC (vpravo) pro pedagogy

Někteří zaměstnanci TUL vlastní čipové klíčenky nebo zaměstnanecké čipové karty. Ty fungují na stejném principu jako tyto čipové karty ISIC/ITIC. Jedná se o čipové karty typu Mifare Classic 4K[2]. Na obrázku číslo 5 je vidět výstup softwaru NFC TagInfo.

2 Data byla načtena mobilním telefonem Samsung Galaxy SIII přímo z čipové karty za pomocí technologie NFC a softwaru NFC TagInfo od NFC Research Lab Hagenberg.



Obrázek 5: Výstup z programy NFC TagInfo

2.2.2 Analýza rizik

Možné bezpečnostní riziko vzniká při ztrátě identifikační čipové karty. V případě, že má student povolený vstup na koleje, může majitel čipové karty vstupovat libovolně do prostoru kolejí. Na čipovou kartu ISIC/ITIC je možné si nechat nahrát aplikaci pro Libereckou veřejnou dopravu. Dále je na kartě kredit do Menzy, a kredit pro tisk. Čipovou kartu ISIC/ITIC je možné využít k vypůjčení si knih a jiného materiálu z Krajské vědecké knihovny Liberec.

Na kartě ISIC Student jsou vytištěny informace o studentovi: jméno, příjmení, datum narození, název univerzity, identifikační číslo studenta, ID ISIC karty (využitelné při slevách).

Na řešení tohoto rizika se aktivně pracuje. Připravuje se nové webové rozhraní pro změnu centrálního hesla. Právě zde bude možnost si zablokovat identifikační kartu v případě její ztráty. Pro opětovné povolení karty (při úspěšném nálezu) je nutné navštívit studijní oddělení, případně karetní centrum, kde kartu znovu odblokují. Odblokování bude možné pouze pro prokázání totožnosti, že karta je u oprávněného držitele.

2.3 Důkaz vlastností

Poslední metodou je využití biometrické ověření identity uživatele. Příkladem biometrického ověření je například: záznam obličeje kamerou, otisk prstů, otisk oční sítnice, hlasový projev (přečtení určité fráze).

Tato metoda také není nejspolehlivější. Podle knihy Počítačová bezpečnost a ochrana dat[1] může dojít ke dvěma chybovým stavům – stav, při kterém bude jako autorizovaný uživatel označen ten, který nemá přístup k systému (FAR – False Acceptance Rate) a stav kde oprávněný uživatel nemá povolený přístup (FRR – False Rejection Rate). Každá tato chyba má svůj vlastní prahový limit, kdy k chybě dojde. Záleží na systému, který zabezpečuje., případně, který se používá. Dále v knize uvádějí příklad kdy se jaký systém hodí.

Pokud chceme, aby bezpečnost byla na co nejvyšší úrovni, je pro nás nepřijatelné, že by systém povolil přístup neautorizované osobě. Je přijatelné, pokud systém odmítne ověřit uživatele, kteří mají mít přístup do systému. Využití FRR. Naopak v závodní jídelně můžeme tolerovat výdej obědu neznámému člověku. Ale strávník by nebyl spokojen v případě, že má nárok na výdej, ale oběd mu nebyl vydán. Využití FAR.

2.3.1 Stávající situace na TUL

Tento typ ověření není možné aplikovat na TUL z důvodu ochrany osobních údajů. TUL není oprávněna shromažďovat biometrické údaje o studentech nebo zaměstnancích.

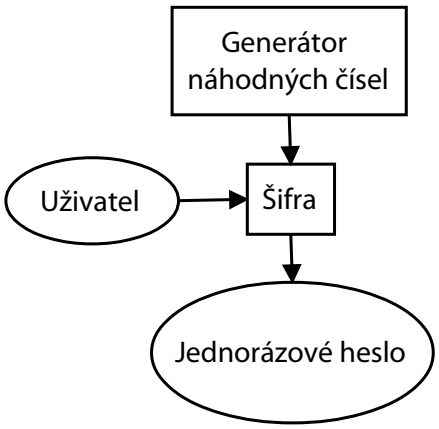
2.4 Kombinace metod

Pro zvýšení bezpečnosti se využívá kombinace výše uvedených metod. Síla zabezpečení systému je ve zvyšování pravděpodobnosti, že nenastane určitá situace. Kreditní karty využívají důkaz znalostí a důkaz vlastnictvím. Kde důkaz znalostí je PIN a důkaz vlastnictvím je kreditní karta, kterou používáme při výběru z bankomatu.

2.5 Různé sdělovací kanály

Další možností zvýšení zabezpečení systému je zvolení různých sdělovacích kanálů pro interakci s uživatelem. V posledních letech se hodně využívá například v bankovnictví. Mám osobní zkušenost s bankovním účtem od Československé obchodní banky, která pro přístup do systému využívá vygenerované **jednorázové** heslo. Jednorázové heslo je uživateli zasláno prostřednictvím textové zprávy na

mobilní telefon.



Obrázek 6: Generování jednorázového hesla [1]

3 Změna centrálního hesla

Osobně jsem si vyzkoušel stávající systém změny centrálního hesla na studijním oddělení Fakulty mechatroniky, informatiky a mezioborových studiích.

Den před návštěvou studijního oddělení, jsem si z bezpečnostních důvodů měnil centrální heslo. Bohužel jsem nové heslo nezměnil na chytrém telefonu, a došlo k zablokování účtu. Systém TUL vyhodnotil, že se někdo snaží uhodnout mé heslo hrubou silou. Proto jsem se celý večer nebyl schopný připojit k internetu.

Následující den jsem přišel na studijní oddělení s ústní žádostí o změnu centrálního hesla. Byl jsem vyzván k nahlášení jména a příjmení. Následně mi bylo vygenerováno nové heslo s omezenou platností.

Před generováním nového hesla, jsem měl být dotázán na občanský průkaz, nebo nějaký jiný osobní doklad s fotografií.

Po konzultaci s panem Petrem Adamce, který pracuje na Oddělení správy sítě LIANE, jsem zjistil, že každý rok pan Adamec rozesílá e-mailem na studijní oddělení informace pro studenty, jak mají nakládat s přístupovými údaji.

Dále také pan Adamec v e-mailu uvádí, že studijní oddělení mají měnit hesla **pouze** až po předložení studentského průkazu, občanského průkazu, atd.

V tomto případě došlo k selhání autentizace uživatele do centrální sítě LIANE.

4 Rešerše systémů jiných univerzit

Komunikoval jsem s panem Ing. Janem Havlíčkem z Vysoké školy ekonomické v Praze (VŠE). S panem Ing. Jiřím Slaninou z Univerzity Pardubice (UPCE). A v neposlední řadě s panem Ing. Pavlem Poláčkem z Univerzity Jana Evangelisty Purkyně (UJEP).

Obrázek 7: Logo VŠE, UJEP a UPCE

4.1 Soubor otázek

1. **Jakým způsobem získávají noví studenti uživatelské jméno a heslo, když nastoupí poprvé na univerzitu?**

   VŠE: V případě, že si uchazeč podá přihlášku elektronicky ve studijním informačním systému (ISIS), poté jim automaticky vzniká speciální typ účtu, který se při přijetí transformuje na standardní účet. Při následné změně hesla v ISISu se toto heslo propíše i do Microsoft Active Directory. V případě, že se někdo ke studiu přihlásil mimo ISIS (papírová přihláška), musí po přijetí osobně na Centrum podpory uživatelů.

   UPCE: Studenti při zápisu obdrží kartu. Kartu mohou přiložit ke snímači, aplikace jim resetuje předvolené heslo a na mini tiskárně jim vyjede nové vygenerované heslo do domény UPCE i k e-mailu Google.

   UJEP: Studenti mají vygenerované heslo podle formátu X<rodné_číslo> do IS/STAG. Pomocí tohoto konta si pak mohou změnit heslo do bezdrátové sítě,

sítě na koleji a k webovým službám (EDUID, e-learning).

2. **K jakým systémům/aplikacím mají studenti s těmito údaji přístup?**

   VŠE: Studijní systém ISIS; Microsoft Active Directory (všechny počítače na VŠE); další WWW služby, ověřující se prostřednictvím LDAP; SMTP server školy; Office 365. Dále je ještě v provozu RADIUS server pro ověření EduROAM a VPN, heslo je oddělené a nesmí být stejné. Nastavuje se prostřednictvím WWW stránky, ověřuje se heslo do ISISu.

   UPCE: Jedná se o řadu informačních systémů, jednotně je evidují jako JIS (Jednotný informační systém). Například se jedná o systém knihovny, intranetu, moodle, e-learning, virtuální laboratoře atd.)

   UJEP: Studenti mají přístup k IS/STAG, webmail.

3. **Jakým způsobem si studenti mohou změnit své heslo?**

   VŠE: Změna v ISISu, změna se propíše i do AD a LDAP. Heslo na RADIUS server se nastavuje skrze WWW stránku.

   UPCE: Změnu hesla provádějí studenti na WWW stránce.

   UJEP: V systému IS/STAG skrze webovou aplikaci.

4. **Jaké mají možnosti obnovení hesla pokud ho zapomenou?**

   VŠE: Musí se osobně dostavit na Centrum podpory uživatelů, kde jim operátor nastaví nové inicializační heslo, to je následně nutné změnit v ISISu. Heslo na RADIUS server změní přes WWW, pokud ovšem znají heslo do ISISu.

   UPCE: Přijdou na IC (Informační centrum), KC (Kartové centrum) nebo CC (Copy Centrum) a po prokázání totožnosti jim je dovoleno přiložit kartu na snímač, aplikace jim resetuje heslo a na mini tiskárně jim vyjede nové vygenerované heslo do domény upce, i k emailu Google.

   UJEP: Osobní návštěva studijního oddělení, kde ověří studentovu totožnost.

5. **Mají studenti na Vaší univerzitě identifikační kartu (ISIC) nebo klíčenku?**

   VŠE: Ano, čipová karta, ISIC (resp. ITIC pro učitele) jako varianta ale existují i karty bez designu a licence ITCS. Karty jsou placené. Převážná většina studentů volí ISIC. Karty jsou i pro externí čtenáře knihovny a další osoby. Existuje i bezplatná varianta karty bez čipu, její využití je ale velmi omezené a vydají se řádově jednotky kusů ročně.

   UPCE: Mají identifikační kartu stejnou jako zaměstnanci. Na obědy, tisk na tiskárnách, přístupy do učeben a budov, do knihovny. Karty ISIC vydává ISIC na občasném stánku, ale trvale to tu není.

   UJEP: Studenti vlastní identifikační čipové karty ISIC.

6. **Při změně hesla se provádí ověření studenta? Pokud ano, jakým způsobem?**

   VŠE: Operátor ověří totožnost pomocí vhodného průkazu totožnosti (školní karta, OP, pas, ŘP a podobně. Musí se jednat o průkaz s fotografií). Ve speciálních případech, kdy se student nemůže dostavit osobně (je prokazatelně v zahraničí a podobně) se situace řeší individuálně.

   UPCE: Ano, k ověření studenta se využívá OP, případně se dá využít ŘP, pas.

   UJEP: Pro ověření studenta se využívá OP.

7. **Jaké dostanou studenti informace, jak se mají zachovat při ztrátě identifikačního předmětu?**

   VŠE: Při zahájení studia mají hromadné informační schůzky, kde dostanou i stručnou informaci o ID kartách. Ztrátu karty obvykle hlásí osobně na Centru podpory uživatelů. Při ztrátě hrozí zejména zneužití peněz v menze nebo na placeném tisku a kopírování.

   UPCE: Ztrátu mají neprodleně hlásit na IC.

UJEP: Při předání karty podepisují studenti papír o předání, který je explicitně neinformuje, co mají dělat v případě ztráty. Tyto informace jsou uvedeny na webových stránkách.

8. **Existuje na Vaší univerzitě služba, která by měl dostupnost 24 hodin denně, kterou by mohli studenti využít v případě zapomenutí hesla a nebo ztrátě identifikačního předmětu?**

   VŠE: Neexistuje.

   UPCE: Ne, jen v pracovní době na IC (Informační centrum), KC (Kartové centrum) nebo CC (Copy Centrum).

   UJEP: Neexistuje.

9. **Jaká pravidla vyžadujete pro tvorbu nového hesla? Počet znaků, velikost písmen, alfanumerické znaky, případně nějaké speciální znaky? Pokud ano, můžete uvést které, případně jejich počet?**

   VŠE: ISIS a AD minimálně 9 znaků, kombinace malých, velkých písmen a číslic. RADIUS min. 8 znaků, kombinace minimálně malých a velkých písmen nebo kombinace písmen a číslic.

   UPCE: Heslo musí obsahovat minimálně 3 typy znaků a minimálně 8 znaků. Heslo se nesmí použít stejné, jako 3x v minulosti.

   UJEP: Heslo musí obsahovat minimálně 8 znaků.

4.2 Shrnutí

Zjistil jsem, že žádná z výše uvedených univerzit, nenabízí svým uživatelům sítě službu pro změnu centrálního hesla dostupnou 24 hodin. Nejzajímavějším typem generování nového heslo má Univerzita Pardubice s využitím mini tiskárny. Systém, ale není povolen 24 hodin.

V případě vyzrazení uživatelského jména a hesla, dojde na všech univerzitách k

bezpečnostnímu problému. Majitel takto nabitého účtu může měnit nastavení uživatele. Tímto jednáním mohou způsobit veliké škody. Například v případě, že někdo zjistí přihlašovací údaje vyučujícího.

Důvodem bezpečnostního rizika je, že mají uživatelé jedno uživatelské jméno a heslo k více informačním systémům. Jedinou obranou je rychlé nahlášení zcizení uživatelského účtu a jeho rychlá blokace.

5 Koncept autentizace uživatele

Pro návrh prototypového zařízení jsem zvolil kombinaci metod důkaz znalostí a důkaz vlastnictvím. Pro zvýšení bezpečnosti jsem zvolil další sdělovací kanál pro komunikaci s uživatelem. Jedná se o textovou zprávu (SMS), v které bude uvedeno jednorázové heslo (PIN), které bude nutné zadat do systému. Jako důkaz vlastnictví jsem zvolil identifikační kartu TUL, ISIC, ITIC, nebo čipovou klíčenku, které se používají na Technické univerzitě v Liberci.

5.1 Povolení služby vzdálené změny hesla

V případě, že uživatel bude chtít využívat služby zařízení, musí si službu povolit. Povolení této služby se provádí na webové stránce LIANE, kde si může student měnit své nastavení.

Od pana Ing. Igora Kopetschkeho mám informaci ke dni 15. 5. 2014, že vývoj webového portálu se dokončuje. Odkaz přímo na nové webové rozhraní zatím není k dispozici. O této situaci budou uživatelé informováni na webových stránkách sítě LIANE.

V době, kdy uživatel zná své přihlašovací údaje, si tuto službu povolí. Pro povolení musí zadat mobilní telefonní číslo, kam přijde ověřující SMS s kódem, která ověří, zda se jedná o uživatele, který o tuto službu žádá. Uživatel tento kód musí vložit do webového portálu, kde dojde k potvrzení a aktivování služby.

Službu může uživatel kdykoliv opět **deaktivovat**.

5.2 Využití služby pro vzdálenou změnu hesla

V případě, že student zapomene své přihlašovací heslo a má službu povolenou, může využít služeb zařízení.

Postup uživatele:

1. Uživatel přijde k terminálu a přiloží identifikační předmět.
2. Na registrovaný mobilní telefon přijde PIN kód, který uživatel zadá do terminálu.
3. Po úspěšném zadání přijde uživateli na mobil nově vygenerované jednorázové heslo, které má omezenou platnost, a s jeho pomocí se přihlásí na webový portál LIANE, kde provede jeho změnu.
4. Tímto způsobem získá uživatel znovu přístup do systému sítě LIANE.

5.3 Bezpečnostní podmínky, limity

Z bezpečnostního hlediska je každému uživateli povolena pouze jedna vzdálená změna hesla za den. Pokud bude chtít uživatel změnit heslo podruhé za den, musí využít studijní oddělení nebo Správu sítě LIANE.

5.3.1 Pro kód PIN

Pro zadání kódu PIN má uživatel stanovený limit 15 minut. Počítá se s krátkou prodlevou při odesílání SMS zprávy. A možné chyby v přepisování kódu PIN do terminálu. V případě třetího špatného pokusu zadání kódu do systému, dojde k ukončení transakce s uživatelem a danému uživateli bude zablokována možnost tento den si změnit heslo. V tomto případě bude muset jít osobně na studijní oddělení nebo na Správu sítě LIANE pro nové heslo.

Tabulka 1: Podmínky a limity pro kód PIN

Časový interval pro zadání	15 minut
Počet možných zadání	3 krát
Typ generovaného kódu	pouze číslice
Počet míst vygenerovaného kódu	8
Tvar odeslaného kódu (např.)	9204-4838

5.3.2 Pro vygenerované jednorázové heslo

Jednorázové heslo, s kterým se může uživatel připojit do sítě LIANE, je z bezpečnostního důvodu omezeno časovým intervalem 4 hodiny. Po uplynutí této doby si musí uživatel počkat do druhého dne, a nebo se osobně dostavit na Studijní oddělení nebo na Správu sítě LIANE.

Tabulka 2: Podmínky a limity pro jednorázové heslo

Počet znaků	8

Typ generovaného hesla	Alfanumerické znaky, s rozdílnou velikostí znaků spolu se speciálními znaky:
	`@, #, $, /, !, ?, &, ^, \, }, {, [, ], (, )`
	Vynechání podobných si znaků:
	`0, O, o, I, i, L, l, 1`

Délka platnosti	4 hodiny

5.4 Univerzitní SMS brána

Pro odesílání SMS zpráv na mobilní zařízení se do budoucna plánuje s vytvořením univerzitní SMS brány. Podle informací od pana Radka Melzera, který pracuje v Oddělení informačních systémů na Technické univerzitě v Liberci, se ke dni 5. 5. 2014 o realizaci SMS brány stále jedná.

5.4.1 SMS brána pomocí GSM modemu

S využitím GSM modemu můžeme odeslat omezené množství SMS zpráv za minutu. Běžně odesílané SMS zprávy nemají garantovaný čas odeslání. V případě zahlcení sítě může dojít ke zpoždění odeslání SMS zprávy, nebo SMS zpráva nemusí dorazit. Pro návrh zřízení potřebuji využít odeslání a doručení SMS zprávy v krátkém

(garantovaném) čase. Uživatel stojí u terminálu, a čeká na PIN kód případně na vygenerované jednorázové heslo.

5.4.2 SMS brána jako služba

V tomto případě jsme připojení přímo na službu operátora, který nám poskytuje odesílání SMS zpráv v garantovaný čas, s potvrzením, že SMS zpráva byla uživateli doručena.

6 Návrh prototypového zařízení

Jaké jsou požadavky pro navrhovaný systém jsem konzultoval osobně s panem Petrem Adamcem, který pracuje v Oddělení pro správu sítě LIANE.

S panem Ing. Igorem Kopetschkem, který spravuje karetní centrum, jsem řešil problematiku webové služby.

6.1 Definice požadavků

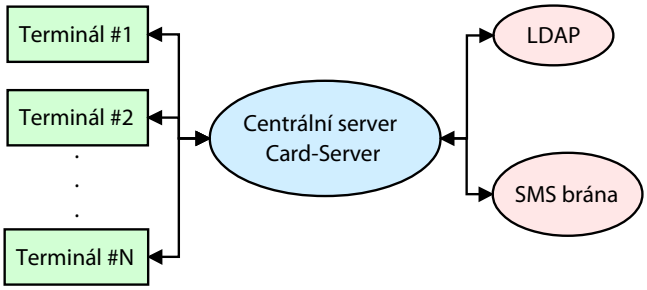
- Jednoduchá a rychlá správa celého systému.
- Možnost snadného rozšíření o další funkce.
- Komunikace mezi jednotlivými systémy musí být šifrována a dostatečně zabezpečena.
- Žádné ukládání vstupních informací od uživatele v systému.
- Komunikace s uživatelem by měla probíhat v několika jazycích. V případě potřeby, možnost doplnění nové jazykové mutace.
- Dostupnost služby 24 hodin denně.
- V případě, že uživatel nebude reagovat na dotazy systému, dojde k přerušení právě prováděné činnosti.
- Snadné přidávání nebo odebírání systémů v síti.

- Nízká pořizovací cena zařízení a nízké náklady na potřebu elektrické energie.

6.2 Návrh systému

Vzhledem k požadavkům, jsem se rozhodl pro volbu centralizovaného systému. Bude k dispozici centrální server Card-Server, který bude navazovat šifrované spojení s jednotlivými terminály.

Tento systém nám umožní jednoduše přidávat do systému nové terminály, a také je ze systému kdykoliv snadno vyřadit. Každý terminál bude identifikován dle jedinečného identifikátoru.



Obrázek 8: Centrální systém

Dále nám centralizovaný systém umožňuje jednoduchou správu aplikace, běžící na terminálech. V případě, že provedeme aktualizaci zdrojových souborů aplikace, můžeme vzdáleně spustit aktualizaci všech terminálů. Nebo můžeme počkat na časový interval, kdy dojde k automatické aktualizaci terminálu. Ta se provádí 1x denně ve 3 hodiny ráno. Aktualizace se také týká slovníků pro jazykové mutace. Jazykové mutace můžeme opět snadno měnit, přidávat nebo ubírat. Stačí pouze definovat, které jazykové slovníky jsou k dispozici v hlavním slovníkovém souboru. V základním nastavení bude k dispozici slovník v českém a anglickém jazyce. Volba jazyka bude úvodní obrazovka, čekající na zahájení interakce od uživatele.

Nevýhodou centralizovaného systému je, že v případě výpadku centrálního serveru tj. Card-Serveru nebude funkční žádný terminál. Jedná se však o doplňkovou službu a i při výpadku stále zůstává možnost obnovy hesla na studijním oddělení nebo oddělení správy sítě LIANE.

6.3 Volba hardwaru a softwaru

V bakalářském projektu „Příprava konfigurace minipočítačů pro výuku“[5] jsem se věnoval výběru zařízení, které má nízké pořizovací náklady, a náklady na provoz zařízení. V práci jsem doporučil zařízení Raspberry Pi typu B. Oproti typu A má ethernetový port, který je v tomto řešení nezbytný. Raspberry Pi odpovídá všem požadavkům, které jsou potřeba pro použití v tomto terminálu.

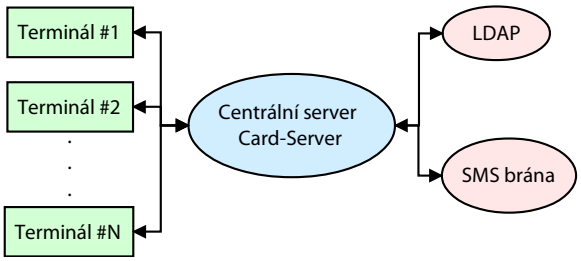
Na Raspberry Pi je možné nainstalovat plně funkční linuxový systém, který požadujeme pro komunikaci s centrálním serverem. Dále nám umožňuje rozšiřovat funkcionalitu terminálu v případě potřeby.

Obrázek 9: Raspberry Pi

Při poškození paměťové karty s operačním systémem stačí, aby technická obsluha na jinou kartu nahrála znovu obraz systému a kartu vyměnila. Jedná se o rutinní servisní postup. Aplikace se z centrálního serveru automaticky stáhne na terminál. Ověří dostupnost veškerých hardwarových periferií a uvede se do provozu.

Obrázek 10: Hardwarová klávesnice

K Raspberry Pi bude připojen monitor s HDMI rozhraním. Dále je kvůli vyšší bezpečnosti systém vybaven hardwarovou klávesnicí. V neposlední řadě je k Raspberry Pi připojena čtečka identifikačních předmětů TWN3 OEM PCB modul Mifare. Tato čtečka bude načítat ID identifikačního předmětu.



Obrázek 11: Schéma komunikace mezi systémy

Terminál bude komunikovat s centrálním serverem s využitím webové služby. Centrální systém dál komunikuje se serverem LDAP, kde jsou uloženy záznamy o přihlašovacích údajích. A bude komunikovat se systémem univerzitní SMS brány.

Webovou službu bude na terminálu ovládat aplikace, která bude napsána v jazyce Python. V základním operačním systému Raspberry Pi jsou předinstalované balíky pro podporu právě tohoto programovacího jazyka. Dále aplikace, která se bude starat o kontrolu aktualizací, aktualizování terminálu, spuštěné hlavní aplikaci (napsané v Pythonu), detekci připojených periferií, případně hlášení výpadků apod., bude napsána v příkazovém interpretu BASH.

Některé části aplikace budou provádět záznamy do textových souborů. Budou pojmenovány jednoznačným identifikátorem terminálu. Soubory se záznamy se budou automaticky zálohovat na server.

Automatické aktualizování terminálu bude vyvoláno pomocí softwarového démona CRON, který je schopen spustit skript, nebo aplikaci v určitý čas.

6.4 Zabezpečení terminálu

Terminály budou pro testování vytvořeny ve dvou provedeních. A budou umístěny do prostorů, které jsou hlídány průmyslovými kamerami. Terminály budou umístěny v budově Menzy Husova, a dále na kolejích Harcov na bloku B.

Terminál bude výhradně připojen k centrálnímu serveru. Centrální server naváže VPN spojení s terminálem.

6.5 Chybová hlášení a stavy

Pro správné zobrazení chybových hlášení na terminálu, je nutné, aby server i terminál měli stejné slovníky chybových hlášení a stavů.

Chybové a stavové hlášení jsem rozdělil na 4 skupiny podle toho, jakou chybu nebo stav označují.

- 1XX – jedná se o chybu lokální, tzn. na terminálu
- 2XX – jedná se o chybu spojenou s uživatelským účtem
- 3XX – chyby znamenající špatné zadání hesel, nebo vypršení určitých limitů
- 4XX – chyby spojené s komunikací se serverem
- 5XX – stavy, které jsou vyhrazeny pro údržbu systému, odstávka terminálů

Tabulka 3: Chybová hlášení a stavy

Číslo chyby	Popis chyby
1	Potvrzovací kód. Vše proběhlo v pořádku.
100	Chyba připojení k síti.
101	Nejsou správně připojené hardwarové periferie.
200	Váš účet neexistuje.
201	Váš účet je blokován.
202	Službu nemáte povolenou.
300	Překročen denní limit pro změnu centrálního hesla.
301	Vypršel časový limit pro zadání kódu PIN.
302	Chybně zadaný kód PIN.
303	Dosažen maximální počet pokusů pro zadání PIN.
400	Síť funguje, ale neodpovídá jeden nebo více závislých systémů.
401	Nastala chyba v odeslání SMS.
402	Došlo k chybě při změně hesla. Heslo nebylo změněno.
500	Terminál je mimo provoz.
501	Právě probíhá aktualizace systému. Prosím čekejte.

6.6 Popis webové služby

Vzhledem k závažnosti procesu, kdy bude docházet ke změně centrálního hesla, nemůžu být připuštěn k práci s tak citlivými daty. Za tuto činnost odpovídá pan Ing. Igor Kopetschke. Po konzultaci s panem Kopetschkem vznikli 3 metody, které stačí pro vzdálenou změnu hesla. Jedná se o:

- ping()
- pinRequest(String chipNr, String readerIdent)
- changePassword(String pin, String ticketNr)

Všechny 3 metody vrací odpověď třídy Status:

- Integer errorCode
- String ticketNr

6.6.1 Význam pojmenování

String chipNr – Jedná se ID hodnotu, která je uložena na čipové kartě a je spárovaná s uživatelským účtem. Při přiložení čipové karty na čtečku, dojde k přečtení této hodnoty.

String readerIdent – Jedná se o jedinečnou hodnotu, která přesně identifikuje terminál, který je připojen do sítě. Podle tohoto čísla server vytvoří tzv. ticket, pod tímto ticketem probíhá další komunikace se serverem.

String pin – Jedná se o PIN kód, který uživateli přišel na mobilní zařízení. Tento kód zadal do terminálu pomocí hardwarové klávesnice.

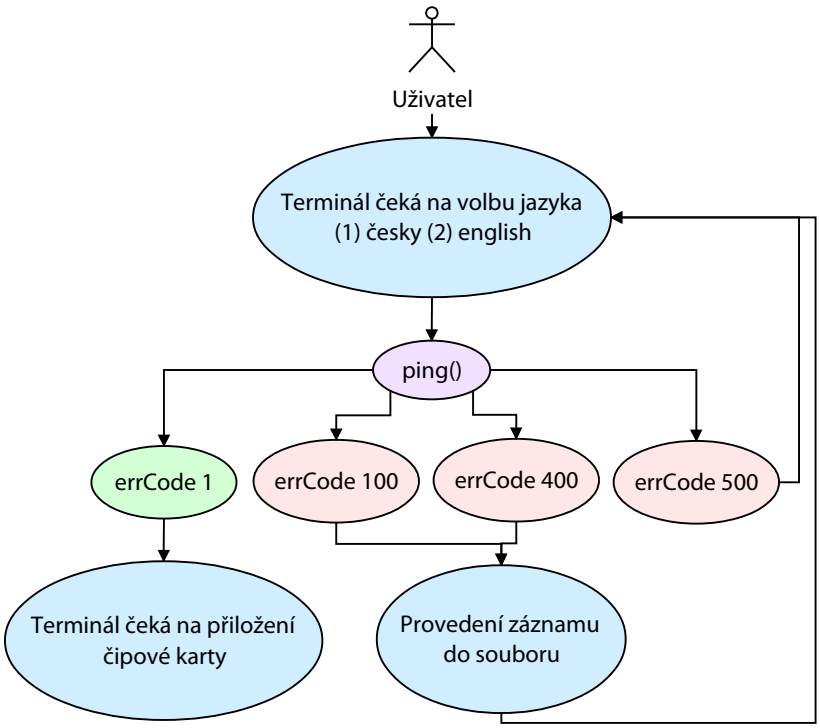
Integer errorCode – Jedná se hodnotu chybové hlášky ze slovníku. Podle této hodnoty se dále chová zařízení, případně i uživatel.

String ticketNr – Jedná se o jedinečnou hodnotu, kterou Card-Server zašle určitému terminálu na začátku komunikace. Začátek komunikace začíná přiložením čipové karty k čtečce. S touto hodnotou pak terminál komunikuje s Card-Serverem do vyřízení požadavku, nebo do vypršení časového limitu.

6.6.2 Metoda ping()

Metoda ping() má na starosti ověření spojení s Card-Server, který dál zjistí, zda všechny propojené systémy fungují.

Metoda ping() nemá žádné parametry, a má celkově 4 možné výstupy.



Obrázek 12: Schéma metody ping()

- **Chybové hlášení errCode 1**

  Terminál ověřil dostupnost centrálního serveru. Centrální server ověřil dostupnost dalších systémů. Jedná se o server LDAP a univerzitní SMS bránu.

- **Chybové hlášení errCode 100**

  V případě, že terminál nemůže navázat spojení s webovou službou, pak se jedná o tuto **lokální** chybu. S největší pravděpodobností je chyba v síti nebo je centrální server nedostupný. Chyba se zapisuje do záznamového souboru.

- **Chybové hlášení errCode 400**

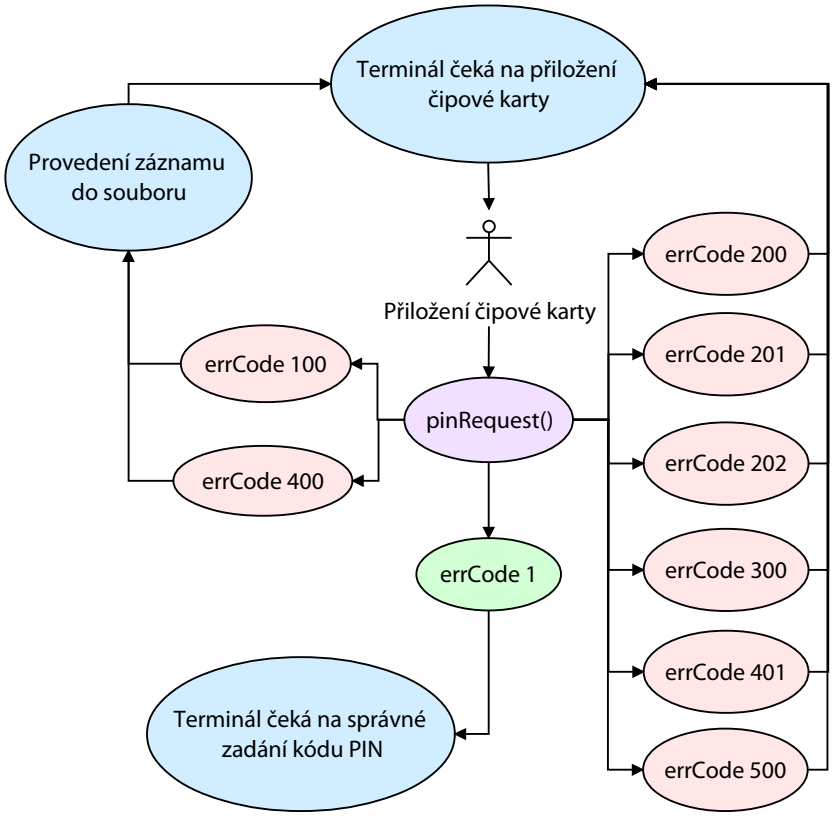
  Centrální server odpovídá. Je možné, že LDAP nebo univerzitní SMS brána provádí možnou údržbu systému, nebo jsou z nějakého jiného důvodu nedostupné. Chyba se zaznamenává do textového souboru.

- **Chybové hlášení errCode 500**

Centrální server odesílá chybu, který každý terminál uvede do stavu „Mimo provoz“. Tato situace je vhodná, při úpravách zdrojových kódů na serveru. Aby nedošlo k nedefinované chybě.

6.6.3 Metoda pinRequest()

K odeslání této metody dojde v momentě kdy, metoda ping() vrátí errCode=1, a dojde k načtení čipové identifikační karty. Parametry této metody jsou **String chipNr** a **String readerIdent**. Metoda vrací devět možných stavů.



Obrázek 13: Schéma metody pinRequest()

- **Chybové hlášení errCode 1**

  Card-Server přijal a úspěšně zpracoval požadavek od terminálu. Card-Server spároval ID karty k uživateli. Zjistil, že má uživatel službu povolenou, že uživatel nepřekročil denní limit pro vzdálenou změnu centrálního hesla a že se úspěšně odeslala SMS zpráva uživateli. Nyní přejde terminál do stavu, kdy čeká na zadání PIN kódu od uživatele. V případě, že uživatel nezadá PIN kód do časového limitu 15 minut, bude transakce automaticky přerušena.

- **Chybové hlášení errCode 200**

  Card-Server nebyl schopen spárovat ID čipové karty s účtem. Z toho vyplývá, že žádný uživatelský účet není přiřazen k této čipové kartě. Proto je nutné, aby uživatel navštívil Studijní oddělení, nebo Oddělení pro správu sítě LIANE.

- **Chybové hlášení errCode 201**

  Card-Server správně spároval ID čipové karty s uživatelským účtem. Ovšem zjistil, že tento účet je z nějakého důvodu zablokovaný. Nemůže dojít ke změně hesla. O této skutečnosti je uživatel informován, a je nutné aby navštívil Studijní oddělení, nebo Oddělení pro správu sítě LIANE.

- **Chybové hlášení errCode 202**

  Card-Serveru se povedlo spárovat ID čipové karty s uživatelem. Účet uživatel nemá zablokovaný. Ale zjistil, že uživatel službu pro vzdálenou změnu hesla nemá povolenou. V tomto případě je nutné, aby uživatel navštívil Studijní oddělení, nebo Oddělení pro správu sítě LIANE, kde si nechá změnit heslo. Do příště si pak službu již může povolit.

- **Chybové hlášení errCode 300**

  Card-Server zjistil správný účet uživatele. Uživatelský účet není blokovaný, má službu aktivovanou, bohužel má vyčerpaný denní limit pro změnu hesla. Musí

tedy znovu požádat osobně o změnu hesla na Studijním oddělení nebo na Oddělení správy sítě LIANE.

- **Chybové hlášení errCode 100, 400 a 500**

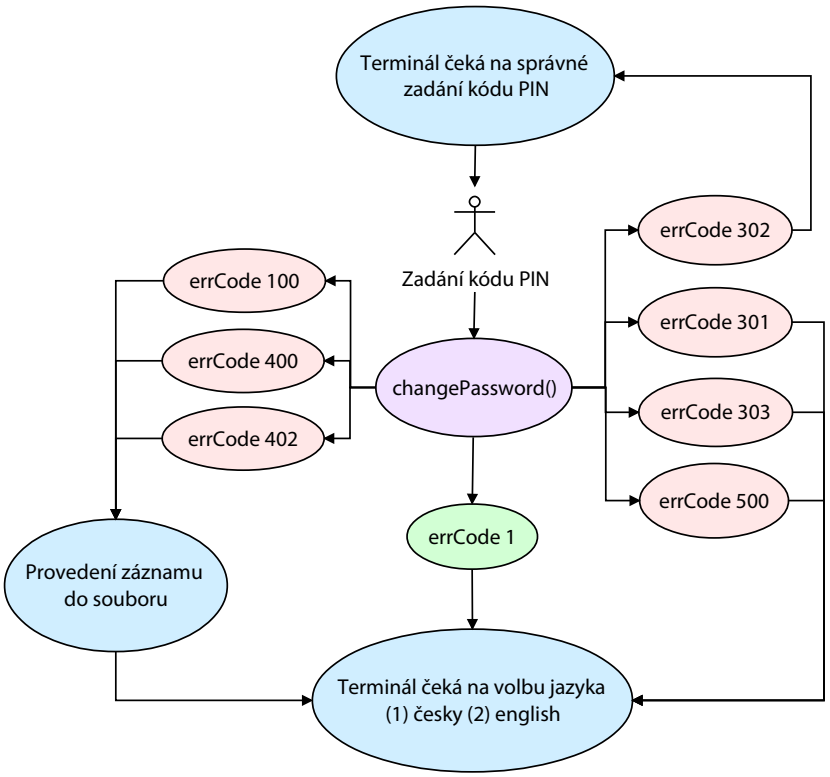
  Je stejné jako v případě metody ping().

- **Chybové hlášení errCode 401**

  Síťové připojení se všemi systému fungují. Nebylo, ale možné vygenerovaný kód PIN odeslat v důsledku chyby na straně univerzitní SMS brány.

6.6.4 Metoda changePassword()

Tato metoda je volána pokaždé, kdy uživatel do terminálu zadá PIN kód a potvrdí odeslání požadavku. Parametry této metody jsou **pin** a **ticketNr**. Tato metoda vrací osm možných stavů.



Obrázek 14: Schéma metody changePassword()

- **Chybové hlášení errCode 1**

  V tomto případě Card-Server ověřil kód PIN. V pořádku se podařilo vygenerovat nové heslo pro uživatele, a zároveň se nové heslo odeslalo uživateli na mobilní zařízení. Nyní má uživatel 4 hodiny na změnu centrálního hesla skrze webový portál pro změnu centrálního hesla.

- **Chybové hlášení errCode 301**

  K zobrazení této chyby dojde v případě, že uživatel odeslal kód PIN po uplynutí časového intervalu pro zadání kódu (15 minut). Chyba je také implementována přímo na terminálu. Z důvodu zvýšení bezpečnosti je nutné, aby tato chyba byla zachytávána také na straně serveru.

- **Chybové hlášení errCode 302**

  Nyní se pokouší uživatel zadat nesprávný kód PIN. Uživateli je snížen počet možných pokusů pro zadání PIN. Terminál čeká na nové zadání kódu od uživatele.

- **Chybové hlášení errCode 303**

  Uživatel ani napotřetí nezadal správně kód PIN. V tomto případě, již uživatel nemá možnost si, v tento den, změnit heslo pomocí terminálu. O této situaci je uživatel informován. Uživatel si může vyčkat jeden den, nebo navštíví osobně Studijní oddělení nebo Oddělení pro správu sítě LIANE.

- **Chybové hlášení errCode 100, 400 a 500**

  Je stejné jako v případě metody ping().

- **Chybové hlášení errCode 402**

  V tomto případě Card-Server ověřil uživatele, služba je povolena, není

překročen časový limit, ani limit pro změnu hesla za den. Ale při změně hesla na serveru LDAP došlo k potížím. V tomto případě nemohla být dokončena změna hesla. Uživatel je o této skutečnosti informován. Tato chyba se zapisuje do záznamového souboru.

7 Závěr

V této bakalářské práci jsem se důkladně seznámil s metodami autentizace uživatele. Navrhl jsem koncept autentizace uživatele s využitím čipové identifikační karty, a zadáním kódu PIN. Ten je uživatelům zadán po jiném sdělovacím kanále než-li po síti. K této komunikaci jsem využil mobilní síť. Kód PIN i jednorázové heslo, s určitou dobou platnosti, jsou uživateli odeslány formou textové zprávy.

Celý systém jsem navrhl centralizovaně. Jednotlivá zařízení fungují zcela automaticky. Stáhnou si aplikaci z centrálního serveru, zkontrolují připojené periferie a uvítají uživatele hláškou s výběrem jazyka. Systém je navržen tak, aby se dali přidávat další jazykové mutace než jen český a anglický jazyk, které jsou v základu.

Je možné zařízení rozšířit například o dotykovou obrazovku.

Na tomto projektu bych rád pokračoval dál i po ukončení bakalářského studia.

Seznam použité literatury

[1] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN: 8025101061.
[2] Centrální heslo sítě LIANE [online]. [cit. 2014-05-16]. Dostupné z: https://liane.tul.cz/heslo/
[3] KeePass Password Safe [online]. [cit. 2014-05-16]. Dostupné z: http://keepass.info/
[4] Shibboleth [online]. 2014 [cit. 2014-05-16]. Dostupné z: https://shibboleth.net
[5] BELDA, Roman. Příprava konfigurace minipočítačů pro výuku. Liberec, 2013. Technická univerzita v Liberci. Vedoucí práce Ing. Lenka Kosková Třísková